AusCERT Remote Monitoring Service (ARMS) User Guide for AusCERT Members

Last updated: 27/06/2014

Contents

1 Introduction 2
1.1 What is ARMS? 2
1.2 Glossary Terms 2
2 Setting up your ARMS configuration (ARM Administrator) 3
2.1 Logging in for the first time 3
2.2 Your Account and Profile 4
2.3 Registered Users and Domains 5
2.3.1 Registered Users 5
2.4 Setting up Contacts 7
2.5 Setting up Hosts 8
2.6 Setting up Service tests 9
2.6.1 Check DNS lookup 9
2.6.2 Ping Host 9
2.6.3 Check a TCP Port 9
2.6.4 Check MX lookups 10
2.6.5 Check Open and Closed TCP Ports 10
2.6.6 Verify the status of an HTTP server 10
2.6.7 Service Name 11
2.7 Notifications 11
3 Managing Service Tests 11
3.1 Dashboard 11
3.2 Alerts 12
3.2.1 Acknowledging the alert 12
3.3 Notifications 13

3.4 Mutes 14
3.5 Logout 15
4 Managing your account (ARM Host Maintainer) ..... **Error! Bookmark not defined.**
5 Managing alerts (ARM Acknowledger) ..... **Error! Bookmark not defined.**
6 Troubleshooting 15
7 AusCERT Technical Support 15
8 Sitemap 15

1 Introduction

1.1 What is ARMS?

AusCERT provides a remote network monitoring service for AusCERT Members (known as **AusCERT Remote Monitoring Service or ARMS)** which sends alerts when hosts and services are not working as expected. It can be configured to monitor host availability, HTTP status, email servers, web servers, DNS checks and host ports on member domains accessible to the internet. Network and System administrators can be notified as soon as there is a problem giving them a chance to fix any issues before users report problems.

The system is designed to be self-configured and requires an active login account for registered Member users (referred to as a registered ARMS user) which is provided as part of the AusCERT Membership. A series of network tests are available to be configured once hosts and contacts are set up. If the tests detect a problem with a host, an alert will be sent by email and/or SMS to the nominated contact/s. The alert needs to be acknowledged by logging in to ARMS. Once the system is recovered, the tests will automatically return to normal.

1.2 Glossary Terms

Member – an AusCERT Membership account.

Registered ARMS User or **User** – an individual nominated by their organization to be a registered AusCERT Member contact for configuring and/or using the ARMS account. Each user will be provided with their own login and allocated one of three roles: Member Administrator, Member Host Maintainer or Member Acknowledger. Within ARMS, a user may have more than one contact depending on how they wish to have the ARMS notifications delivered for each host.

Registered ARMS Domain or **Domain–** a primary fully qualified domain provided by the Member as part of their AusCERT Membership account.

Host – a registered domain or subdomain of a registered domain to be monitored. This must be accessible over the internet.

Contact – a contact email and/or SMS number to which the ARMS notifications are sent.

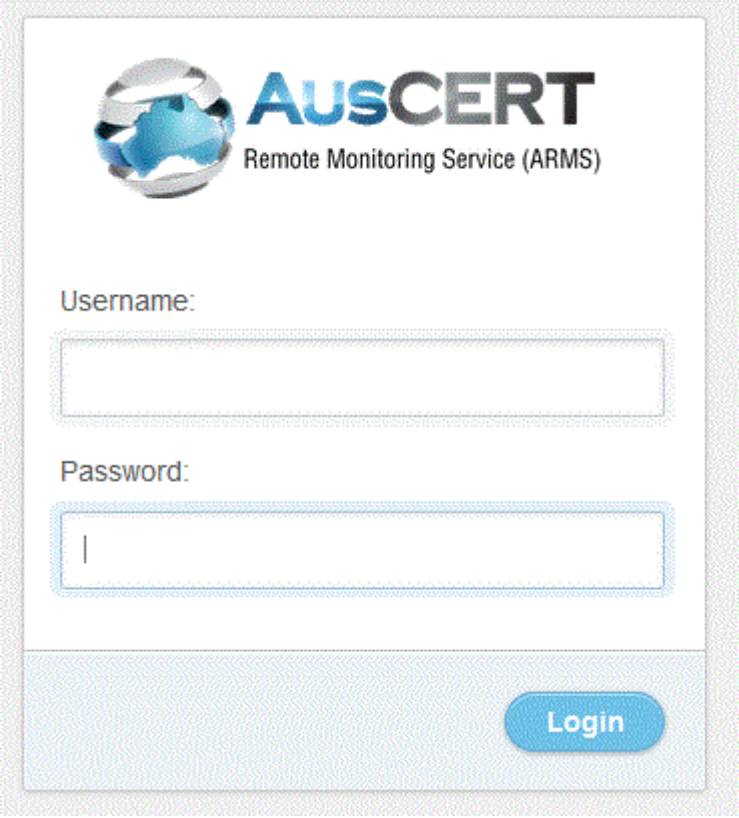
Member Administrator – a user who has been allocated a role in administering the ARMS account. They are able to add hosts to the system for monitoring, set up tests on those hosts and add contacts to the system to receive the ARMS alert notifications. In addition they are able to acknowledge the alerts (ie, turn them off) and remove hosts, tests and contacts from the ARMS account.

Services – These are the tests which check for host availability and integrity.

2 Setting up your ARMS configuration (ARM Administrator)

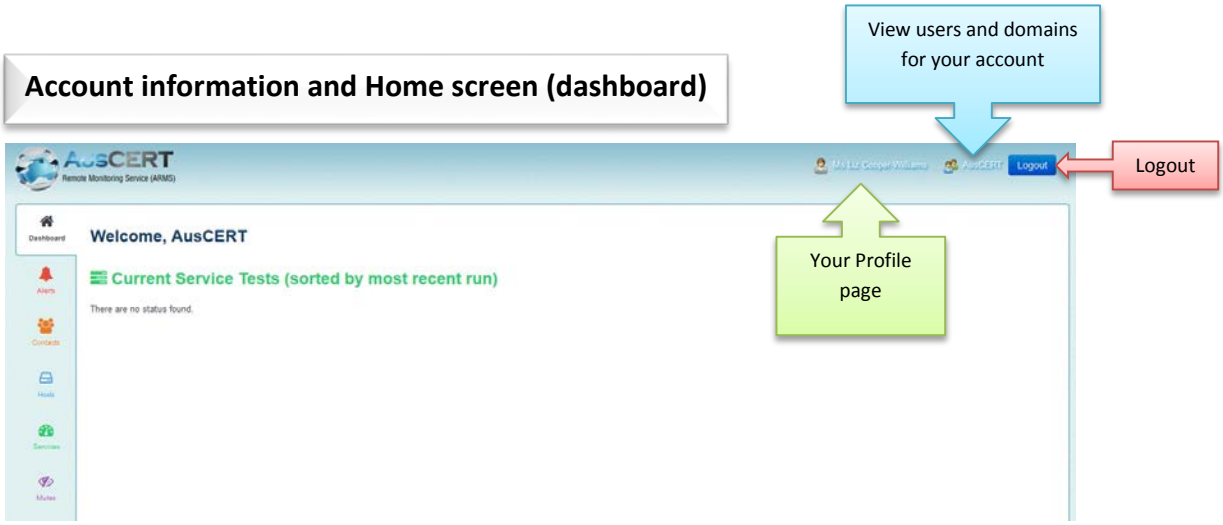
2.1 Logging in for the first time

Login via the URL: https://arms.auscert.org.au



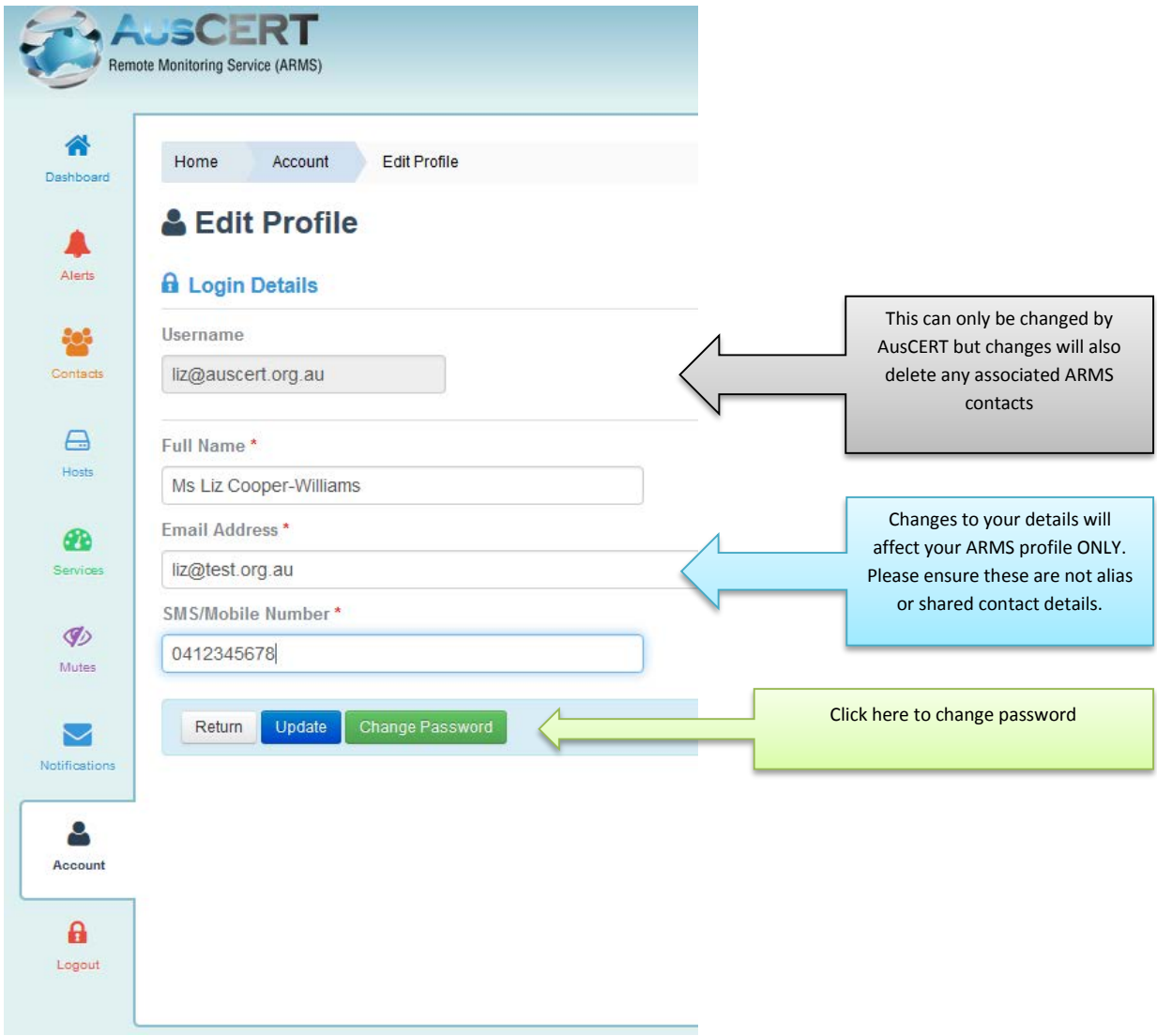
The AusCERT Membership team will issue you with an ARMS username and password for your AusCERT Membership account.

If you have forgotten your username or password or if there are any difficulties with logging in, please contact the AusCERT Membership team.



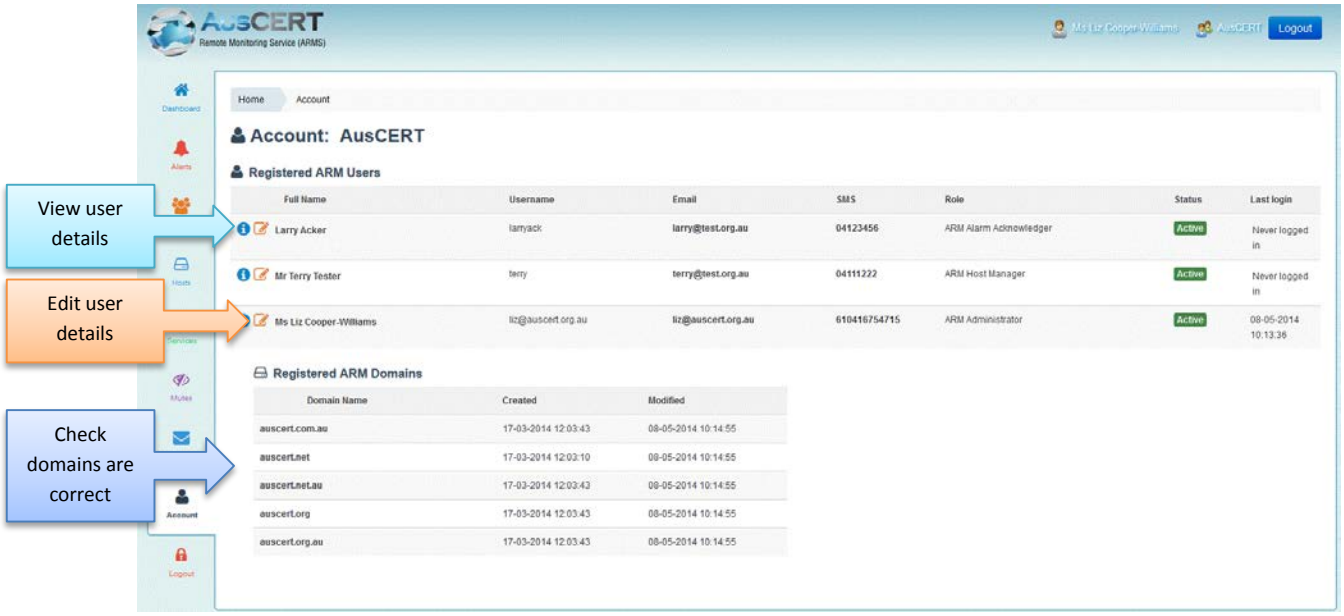
2.2 Your Account and Profile

Once successfully logged in, you should go to your Profile page where you can reset your password and change your display name. Your email and mobile number can also be changed here but please note that these are only used to **verify your identity** and should not be a group alias email or shared mobile.



2.3 Registered Users and Domains

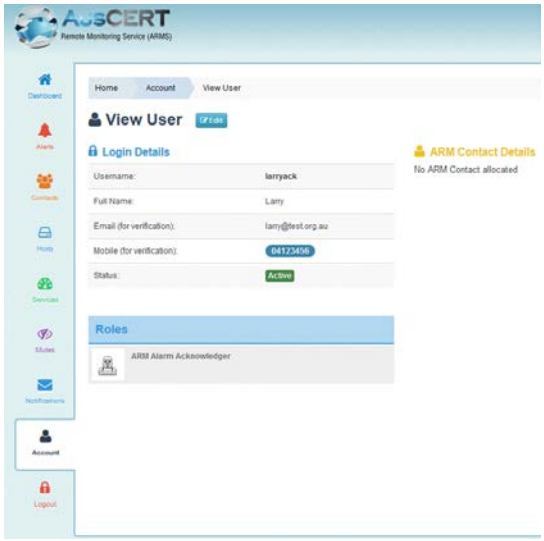
To check your account has both registered users (for adding contacts) and domains (for adding hosts) select “Account” from the left side menu or your organization name from the top right. If users and or required domains are missing, please contact AusCERT Membership directly. Note that not all your Membership domains may have been requested for this service.



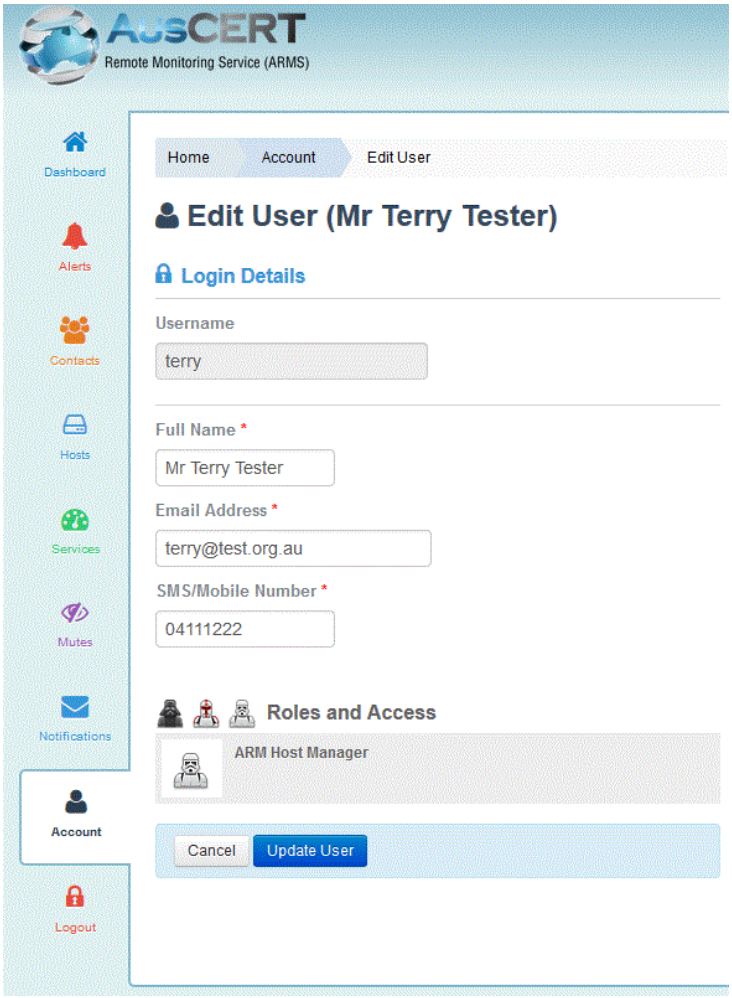
2.3.1 Registered Users

The registered users are those people nominated to use the ARMS account service in the AusCERT Membership agreement. They will each be provided with a login account. As an administrator, you can edit their login details if necessary.

To **view a user’s details** – click on the blue “I” icon in the user list. This will also show any contacts linked with this user (ie, contact details for ARMS) – see next section.



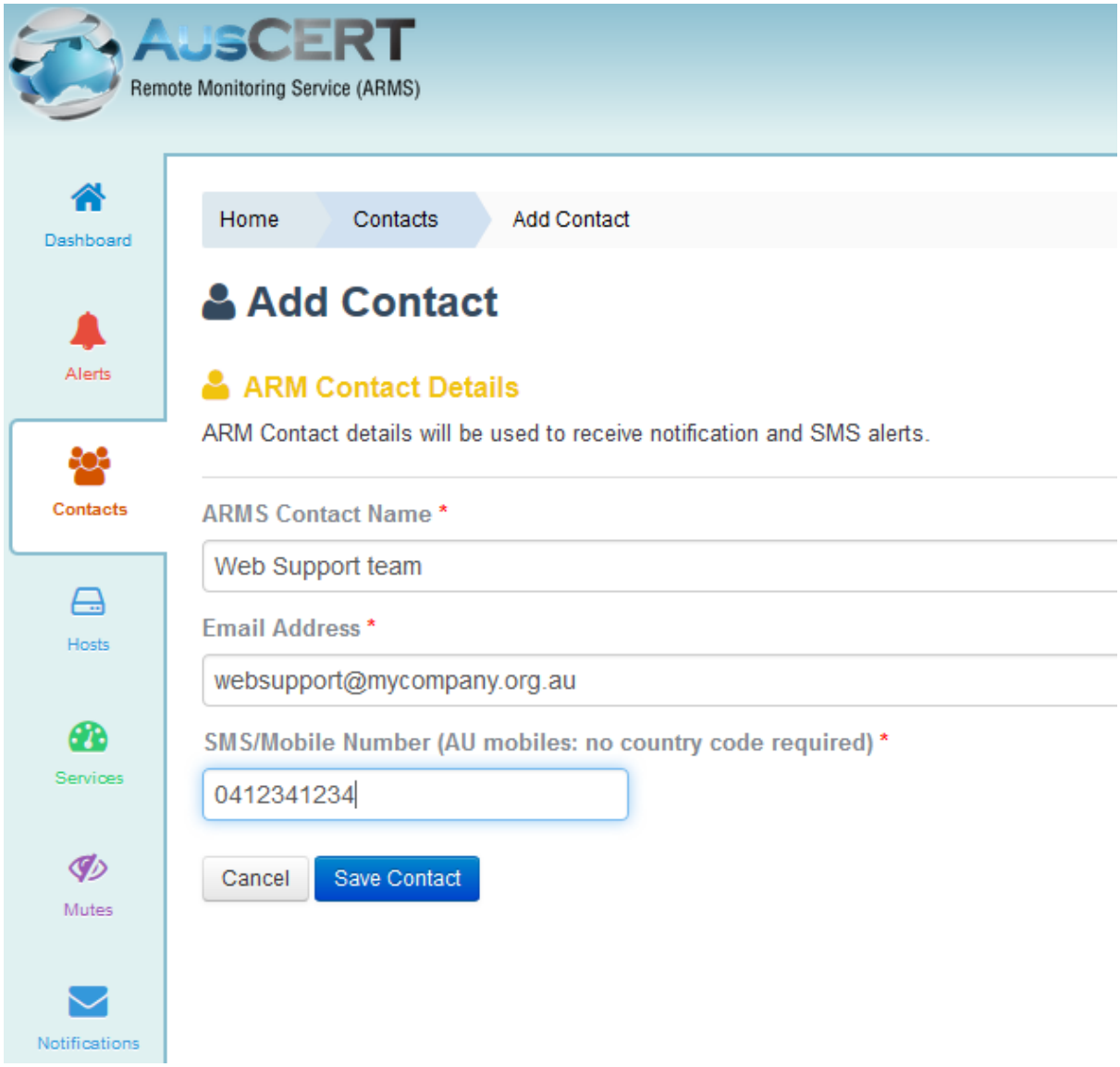
To **edit a user's details** – click on the Edit button from the View page or the orange edit icon from the User list. Note that the email and mobile numbers provided here will **not** be used by ARMS acknowledgments.



To **change another user's password** – currently, a request must be made to the AusCERT Membership team.

2.4 Setting up Contacts

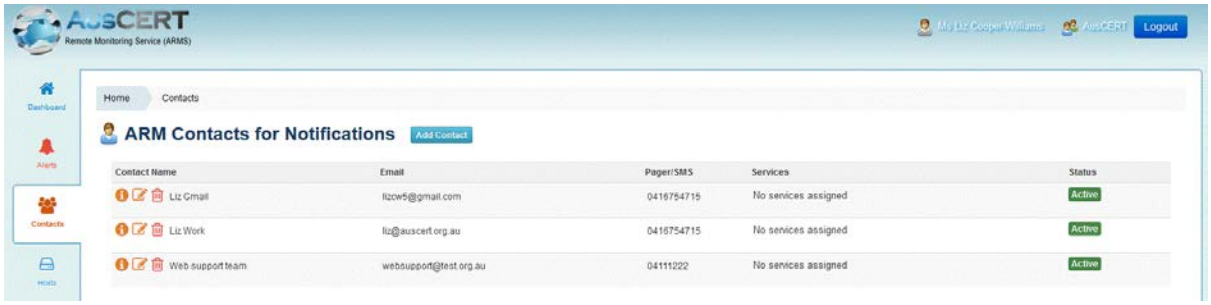
Contacts need to be set up in order to receive notifications from ARMS. **A contact should be an ARMS administrator** already, so that he or she is able to handle alerts sent by the system. Select "Contacts" from the left side menu. Then click on "Add Contact".



1. Enter a name for this contact under "ARMS Contact Name"
2. Enter the email address for this contact – this can be an alias eg., websupport@mycompany.org.au
3. Enter an SMS number – eg company mobile.
4. Click on "Save Contact"

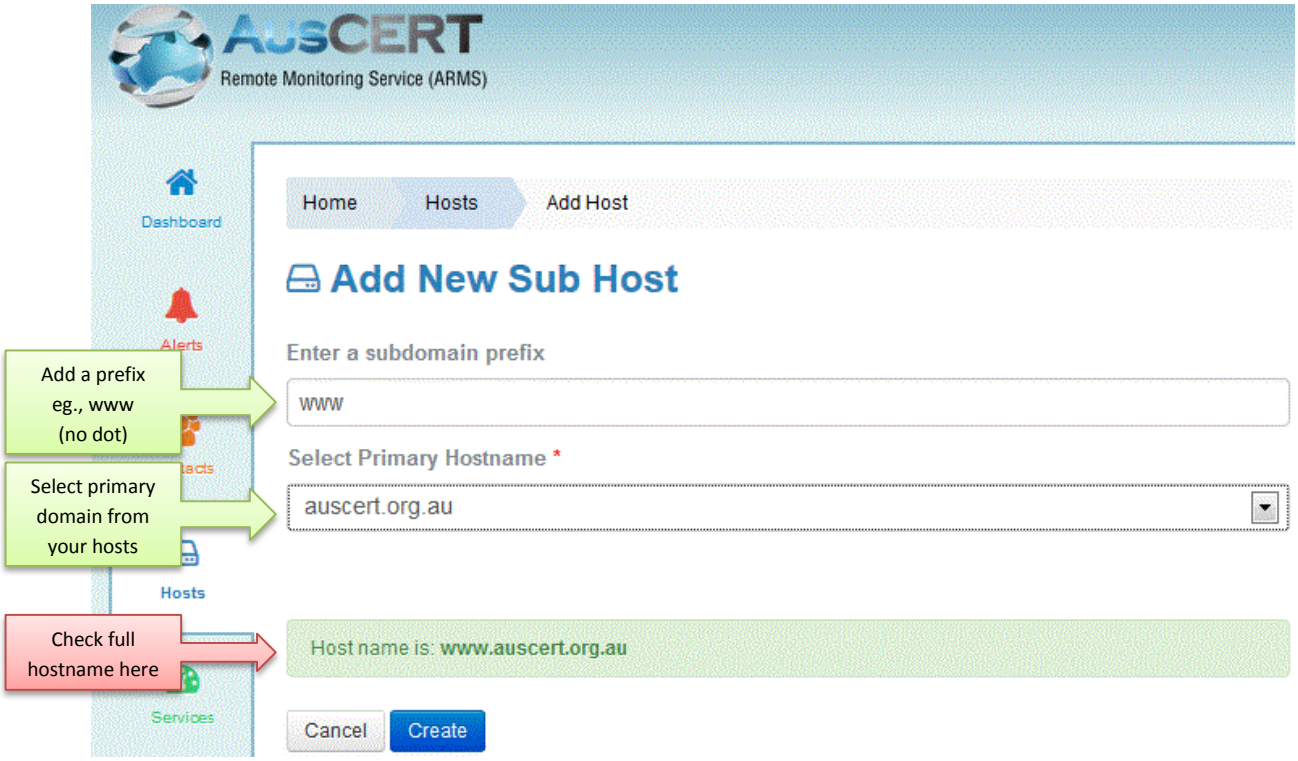
The contact can be viewed, edited or deleted from the contact list. A contact is assigned to a service during its configuration and will receive alerts from that service test if there is a problem.

Contacts are independently managed by AusCERT Members who have been assigned as ARM Administrators.



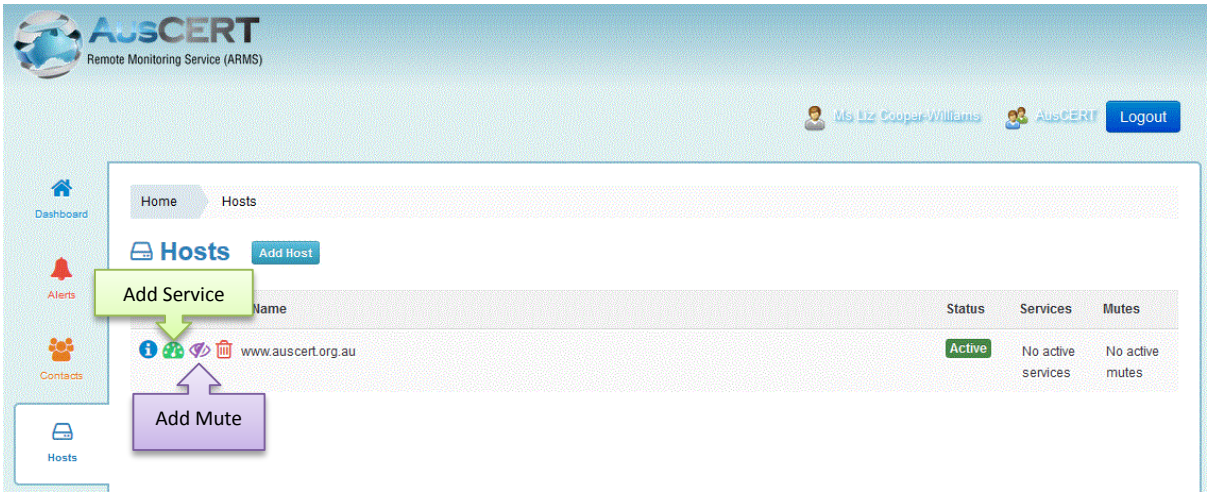
2.5 Setting up Hosts

From the side menu, select “Hosts” then click on “Add Host”.



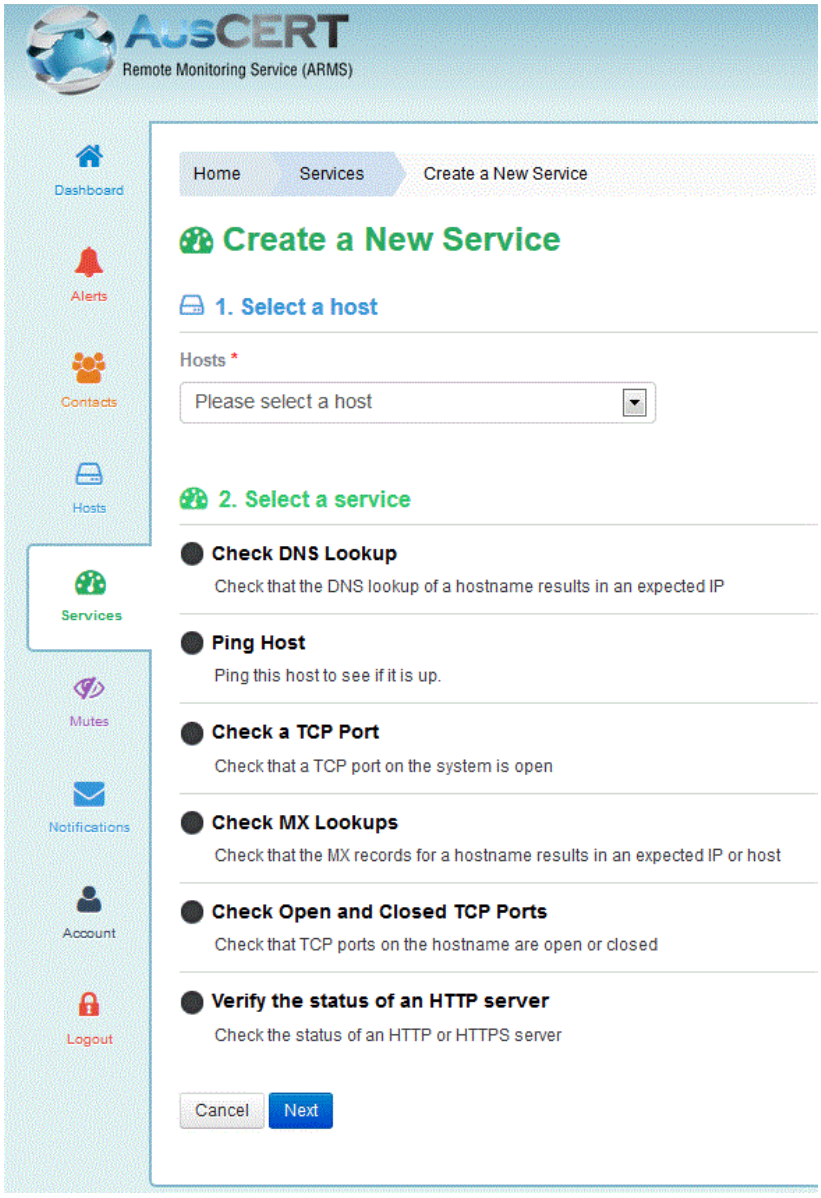
A host can be any domain or subdomain registered as part of your AusCERT Membership account. If the dropdown list “Select a primary hostname” is empty or to add another primary domain, please contact AusCERT Membership directly. **Only use hosts that are visible across the internet, these services will not be able to access any internal hosts**.

Enter the subdomain prefix (if required) and check the “Host Name”. Note it is not necessary to add the final “dot”. If the selection is changed, this will be updated automatically – so if the selection has not picked up the primary selection, please try selecting it again and clicking away from the text boxes. The Host name cannot be edited directly. Click on the “Create” button and this should return you to the Host list page. From here, you can add services and mutes to the host or view host details or delete the host (which has no effect on the primary domain).



2.6 Setting up Service tests

From the side menu, select “Services” then click on “Add New”.


AusCERT
Remote Monitoring Service (ARMS)
Dashboard
Alerts
Contacts
Hosts
Services
Mutes
Notifications
Account
Logout
Home
Services
Create a New Service
Create a New Service
1. Select a host
Hosts *
Please select a host
2. Select a service
Check DNS Lookup
Check that the DNS lookup of a hostname results in an expected IP
Ping Host
Ping this host to see if it is up.
Check a TCP Port
Check that a TCP port on the system is open
Check MX Lookups
Check that the MX records for a hostname results in an expected IP or host
Check Open and Closed TCP Ports
Check that TCP ports on the hostname are open or closed
Verify the status of an HTTP server
Check the status of an HTTP or HTTPS server
Cancel
Next

1. Select a host for the service test from the dropdown list. If your host is not in the list, then return to Hosts and add it as above.
2. Select a service from the list of available services.

The current list of services are:

2.6.1 Check DNS lookup

Checks the IP of a host via DNS lookup. You will need the IP of your host.

2.6.2 Ping Host

ICMP ping test which checks that a host is available across the internet.

2.6.3 Check a TCP Port

A port check test which determines whether a port is open. This is a simple check for an open port. You will need to provide an open port number for your host. For a more advanced check, use Check Open and Closed TCP Ports.

2.6.4 Check MX lookups

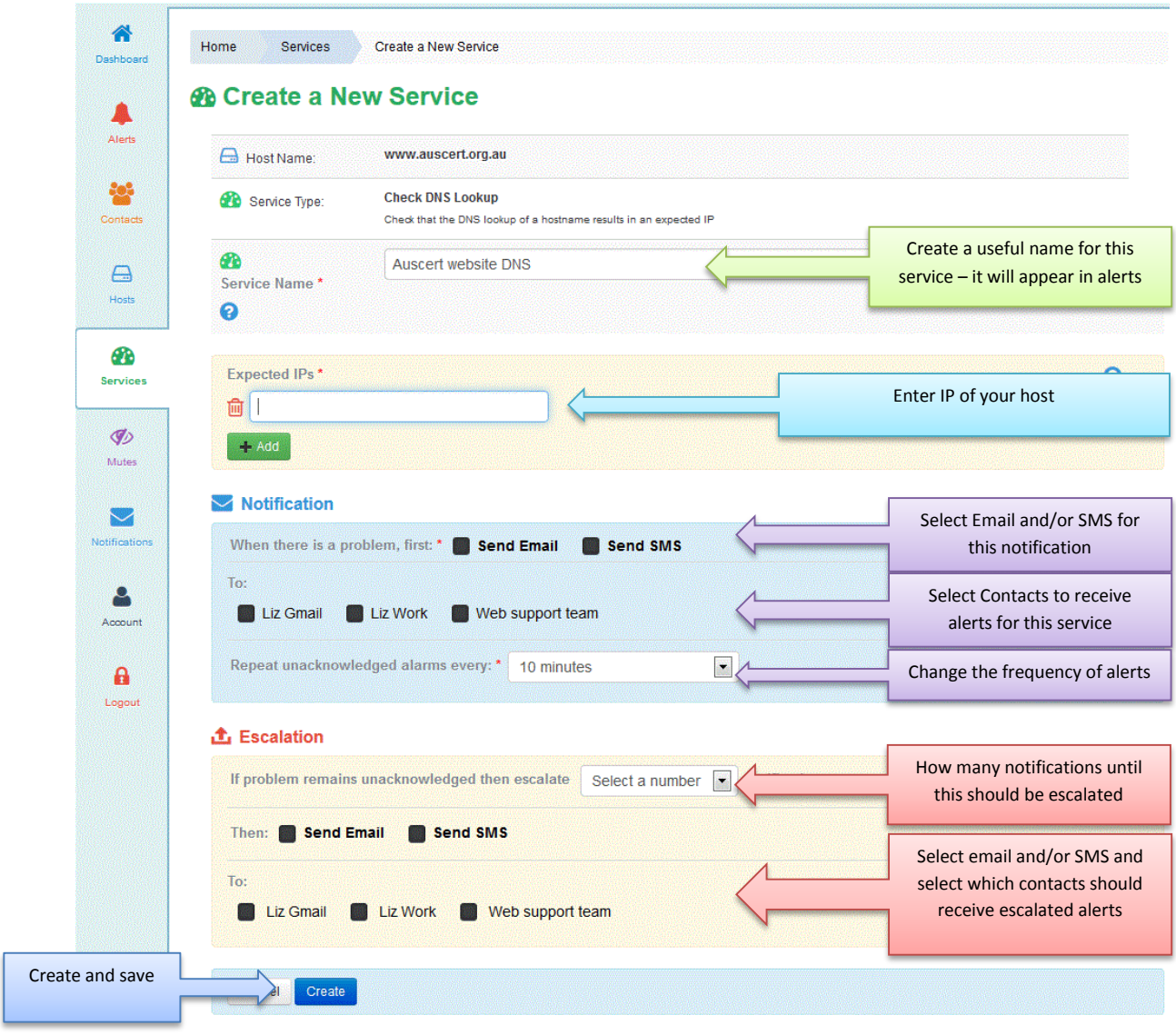
This compares the MX records for a hostname. You will need the full list of MX records for your mail server which can be found here: http://mxtoolbox.com/

2.6.5 Check Open and Closed TCP Ports

A more complex test than the TCP port check, this test accepts multiple ports for both open and closed tests in a single configuration. If one of the ports is not as expected, a warning will be sent for the whole test. You will need a list of open and closed ports that you wish to have monitored.

2.6.6 Verify the status of an HTTP server

This test does an HTTP status check with default ports 8080 (HTTP) and 443 (HTTPS). If yourweb server is running on another port, that can also be specified. The test expects to return an HTTP 200 OK result.



2.6.7 Service Name

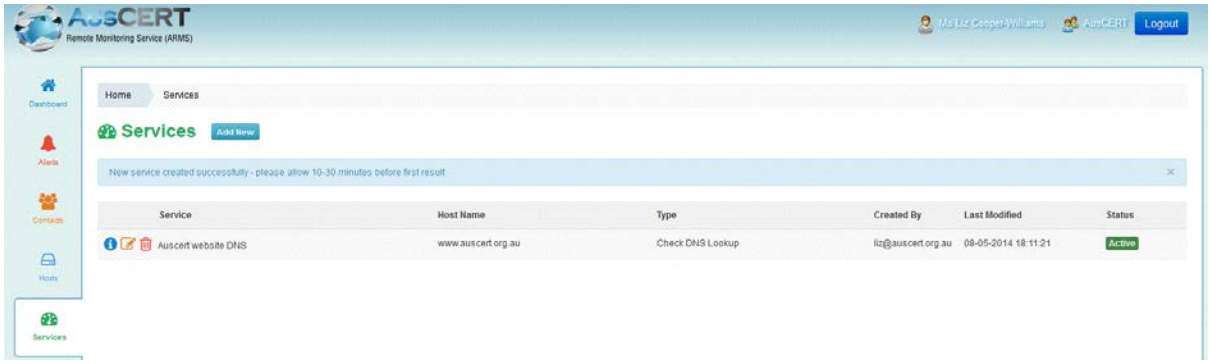
After clicking on “Next”, you will be presented with a form to enter the required data for each test. Each test is identified by a name which you provide – a description of the host and the test is the most useful. This information will assist you identifying which test has failed when you receive an alert. Click on the ? icon for further information.

2.7 Notifications

Check the contact/s who should be notified if there is an alert and whether to send an email and/or SMS. Adjust the frequency of unacknowledged alarms.

Escalations: Check the contact/s who should be notified if the initial alert/s are not acknowledged and after how many notifications this should occur.

Click on “Create” to save the service test details. Please note that there is a delay of 10 to 30 minutes before the first test is run. The service should appear on the Service list page and after a short delay of up to 10 mins, on the Dashboard list as “Pending” which indicates that the details have been loaded but the test has yet to be run. Test results will appear on the Dashboard page and should have an “OK” or green status.

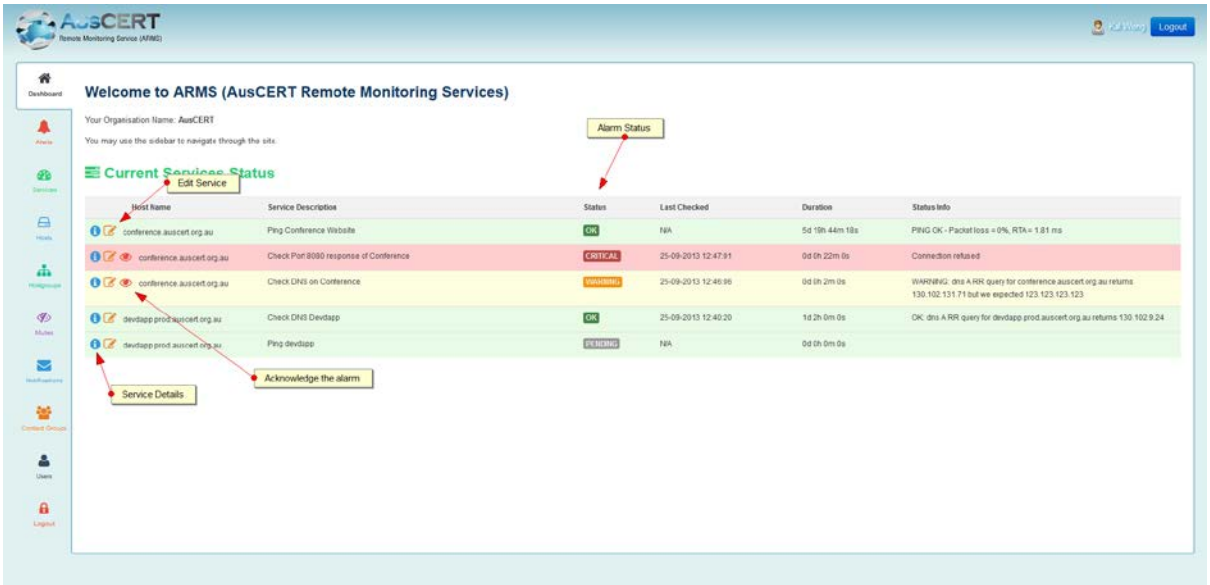


3 Managing Service Tests

Once your ARMS account has been configured with hosts, contacts and services, it will begin actively monitoring your hosts.

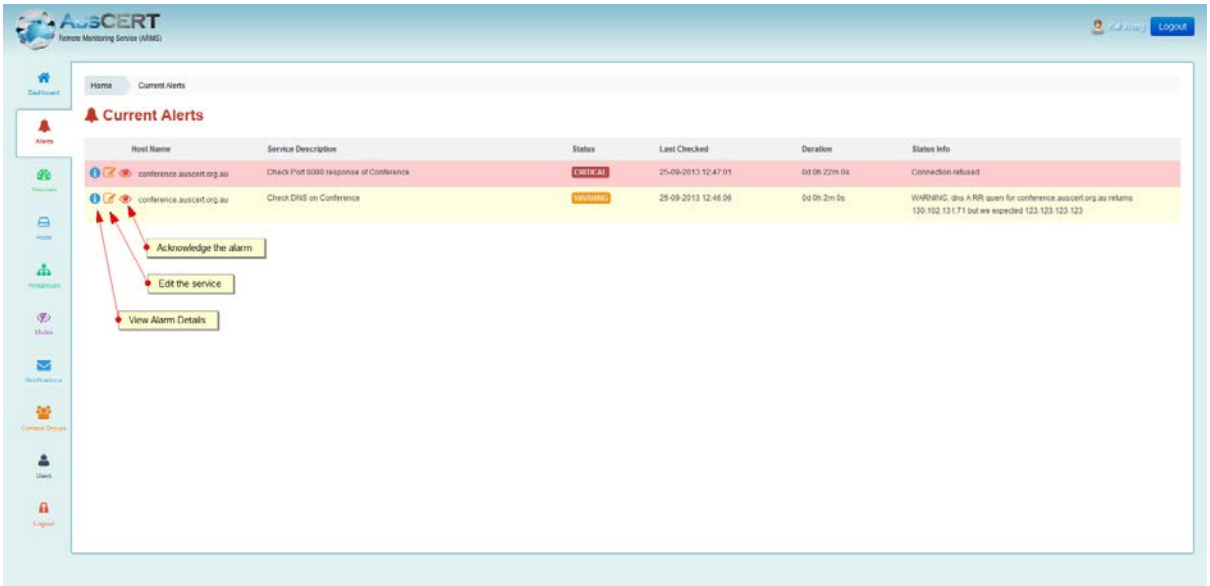
3.1 Dashboard

The Dashboard page shows you the last run and status of all your host tests. If the test has failed, the service is highlighted in red, its status shows as “CRITICAL” and the status info shows the test result. This will have triggered an alert which you should receive as configured in the service test. Some tests may be blocked by your organization’s firewalls and show “Connection not permitted or refused” – these tests should be deleted. Alerts must be acknowledged by clicking on the “red eye” icon.



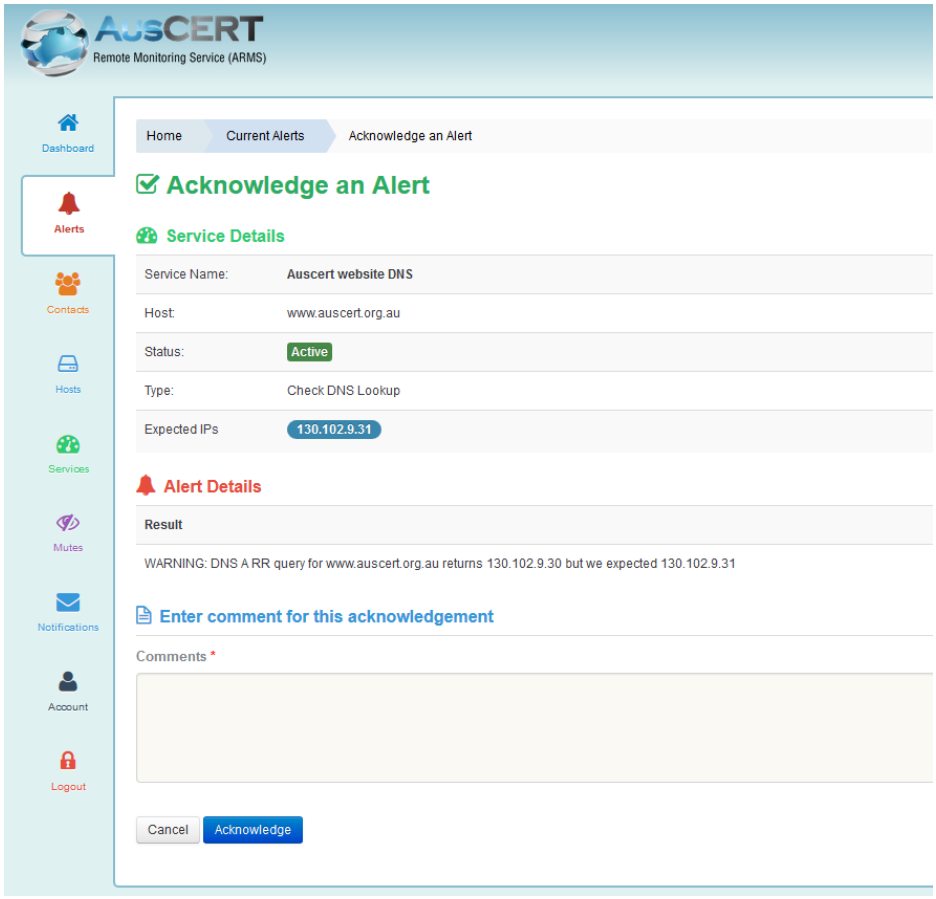
3.2 Alerts

The Alerts page will just show you any tests which have failed and allow you to acknowledge the alert.



3.2.1 Acknowledging the alert

When a test fails, an alert is triggered and this must be acknowledged by the Member administrator, host maintainer or acknowledger by logging into the ARMs website and from here by clicking on the “Acknowledge” icon.



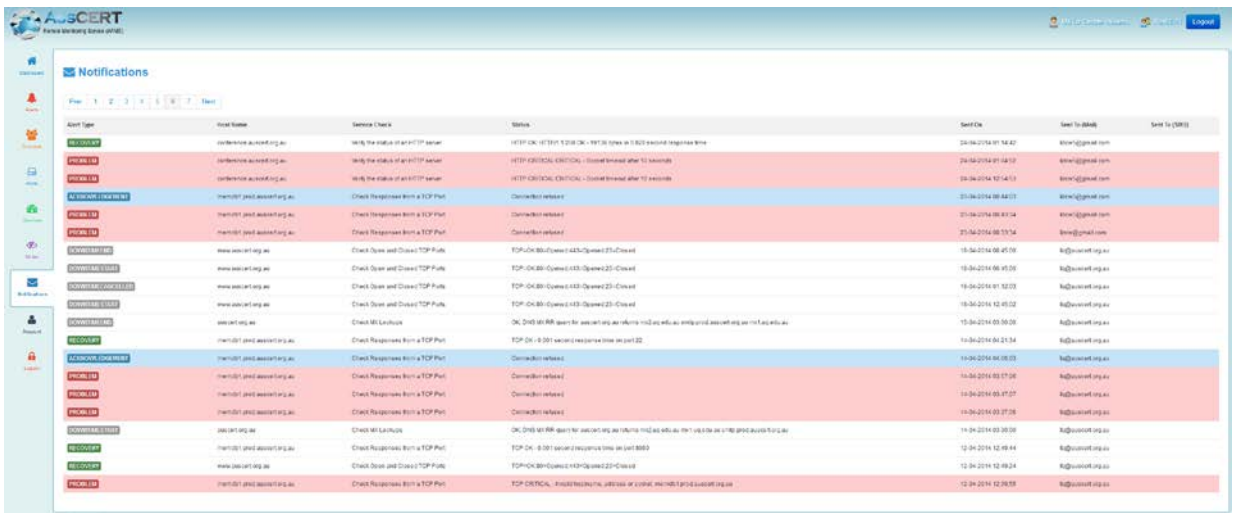
Enter an explanation or comment about the alert for reference and click "Save".

If the alert is not acknowledged, the system will continue to send alerts at the frequency specified when setting up the service test. If the escalation notification procedure has also been set up, this will be triggered when the number of alerts has exceeded the limit specified.

The only way to **silence the alerts** is to acknowledge them. If you have lost your login or are unable to access the website, please contact the AusCERT Technical Support team and they can acknowledge your alert for you.

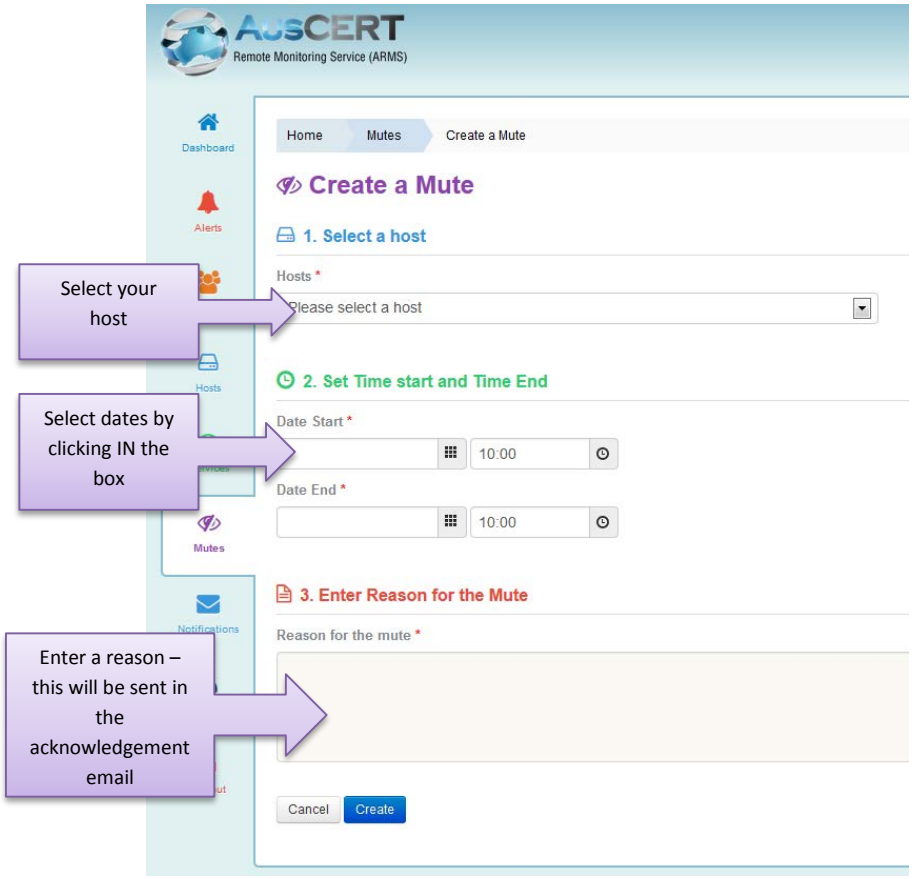
3.3 Notifications

A history of all notifications to your account is shown by clicking on "Notifications" on the side menu. If for any reason, you have not received the notification as shown, please contact AusCERT Membership team and request technical support.



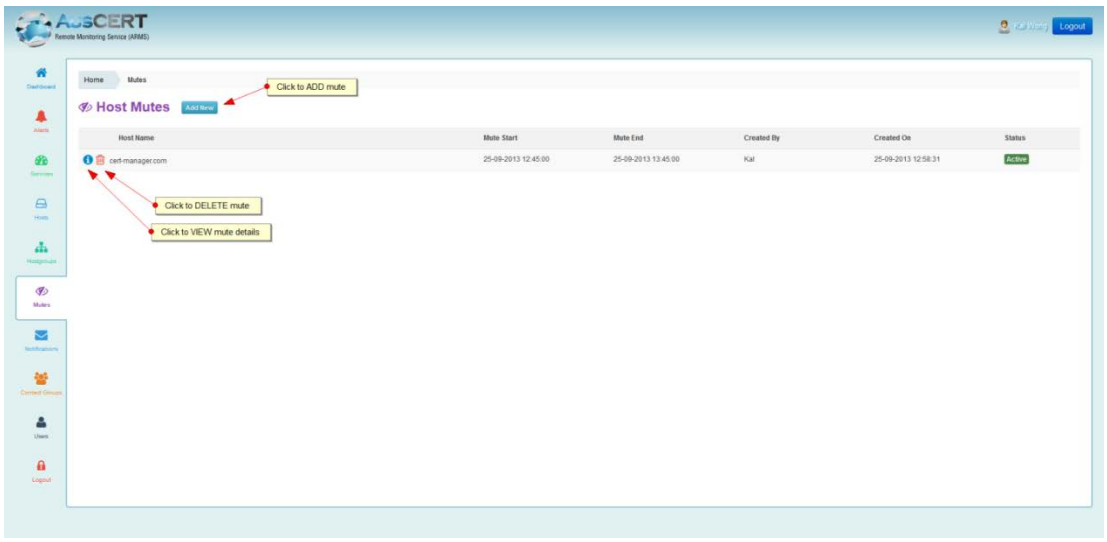
3.4 Mutes

If a downtime for your host is known in advance, the tests can be deliberately muted.



From the side menu, select “Mutes” then “Add Mute”. The tests will continue to run during this period but if they fail, they will not send any alerts. Enter the information as required – to select the date, click **in** the text box. Then click the “Create” button.

Check that the mute appears in the list. It may be cancelled by clicking on the “Delete” icon.



3.5 Logout

Select “Logout” from the bottom of the side menu or top right of the Profile link to ensure you have closed your login session. Your session will timeout automatically after 10 minutes.

4 Troubleshooting

Invalid Host - Host showing as “Unreachable” and/or “Invalid” – this host should be removed as it is either not accessible for remote monitoring over the internet or it does not exist as typed.

Prohibited Host - PING Service showing as “Host Prohibited” – this host should be removed as it is not accessible for remote monitoring over the internet.

No alerts received –

1. Check there is no mute on the host for this period.
2. Check the service has been set up correctly and a contact has been assigned.
3. Check the email and mobile phone numbers for the contact are correct.
4. Check the Notifications list to see if there is an appropriate entry there.
5. Contact AusCERT Technical Support with your account name and contact for further assistance.

5 AusCERT Technical Support

The first point of contact should be a call to AusCERT Membership team on:

Phone: 1800 648 458

Email: membership@auscert.org.au

If this is not available, the AusCERT Technical support team can be contacted directly by email to tech@auscert.org.au

6 Sitemap

ARM Members Interface Sitemap (V.2.0)